



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/720,971	04/06/2001	Olli Immonen	367.39437X00	8278
20457	7590	04/22/2004	EXAMINER	
ANTONELLI, TERRY, STOUT & KRAUS, LLP 1300 NORTH SEVENTEENTH STREET SUITE 1800 ARLINGTON, VA 22209-9889			NORRIS, TREMAYNE M	
		ART UNIT		PAPER NUMBER
		2137		9

DATE MAILED: 04/22/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)
	09/720,971	IMMONEN, OLLI
	Examiner Tremayne M. Norris	Art Unit 2137

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --
Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).

Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) Responsive to communication(s) filed on 03 January 2001.
- 2a) This action is FINAL. 2b) This action is non-final.
- 3) Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) Claim(s) 1-45 is/are pending in the application.
 - 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) Claim(s) _____ is/are allowed.
- 6) Claim(s) 1-45 is/are rejected.
- 7) Claim(s) _____ is/are objected to.
- 8) Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) The specification is objected to by the Examiner.
- 10) The drawing(s) filed on 03 January 2001 is/are: a) accepted or b) objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
 - a) All b) Some * c) None of:
 1. Certified copies of the priority documents have been received.
 2. Certified copies of the priority documents have been received in Application No. DK 1998 000867.
 3. Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892)	4) <input type="checkbox"/> Interview Summary (PTO-413)
2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948)	Paper No(s)/Mail Date. _____ .
3) <input checked="" type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date <u>6</u> .	5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152)
	6) <input type="checkbox"/> Other: _____ .

DETAILED ACTION

Drawings

1. The drawings are objected to as failing to comply with 37 CFR 1.84(p)(5) because they do not include the following reference sign(s) mentioned in the description: "controller 18". In fig.2, the word "processor" was substituted for the word "controller". A proposed drawing correction or corrected drawings are required in reply to the Office action to avoid abandonment of the application. The objection to the drawings will not be held in abeyance.

Specification

2. The disclosure is objected to because of the following informalities: On page 10 line 26 it states "The phone 1 has to delete the from its RAM..."; it is unclear as to what is being deleted. On page 13 line 4, it is unclear as to what "apparatus 20,20,30" corresponds to in fig. 3. Starting on page 14 line 26, the word "respond" needs to be changed to "response". On page 14 line 30, it is unclear as to where the private key is coming from.

Appropriate correction is required.

Claim Objections

3. Claims 13 and 41 are objected to under 37 CFR 1.75(c), as being of improper dependent form for failing to further limit the subject matter of a previous claim. Applicant is required to cancel the claim(s), or amend the claim(s) to place the claim(s) in proper dependent form, or rewrite the claim(s) in

independent form. Regarding claims 13 and 41, smart cards were claimed in the previous claims that they depend from:

Claim Rejections - 35 USC § 112

4. The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

5. Claims 4,26, and 27 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. It is unclear in these claims as to whether the smart card is the separate unit or if there is another separate unit within the smart card.

Claim Rejections - 35 USC § 103

6. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

7. Claims 1,3,19,21-24,27-44 rejected under 35 U.S.C. 103(a) as being unpatentable over Ichikawa (PCT WO 97/24831), and further in view of Anvret et al (EPO 0538216 A1).

Regarding claim 1, Ichikawa teaches a method for establishing a secure connection between a wireless communication apparatus and a data communication apparatus based on a wireless application protocol, wherein said wireless communication apparatus has memory means including a separate unit comprising information to control the access of the wireless communication apparatus through a wireless communication network connected to said data communication apparatus, comprising the following steps (page 1 lines 9-15); :

connecting said wireless communication apparatus to the separate unit, accessing the wireless communication network connected to said data communication apparatus the wireless communication apparatus (page 2 line 16 thru page 3 line 12).

the wireless communication apparatus transmits a request to the data communication apparatus to establish a connection, said request comprising information of which pre-defined algorithm(s) the wireless communication apparatus supports (page 10 line 14 thru page 11 line 11).

upon reception of said request, the data communication apparatus chooses at least one algorithm, and transmits a message back to the wireless communication apparatus, said message comprising the information about which algorithm the data communication apparatus has chosen (page 9 lines 13-23),

upon reception of the message, the wireless communication apparatus generates a master secret code (page 4 lines 10-12), and calculates a signature based on the chosen algorithm and the master secret code (page 4 lines 12-15),

saving said master secret code on said memory means and in the data communication apparatus, in order to re-establish the connection at a later occasion (page 7 line 3 thru page 8 line 4).

What Anvret et al teaches that Ichikawa does not teach is the usage of public (col.6 lines 1-11) and a private keys (col.6 lines 47-48) in message communication,

transmitting a message to the wireless communication apparatus, said message comprising the public key (col.6 lines 39-41),

transmitting a response to the data communication apparatus, said response comprising the calculated signature (col.6 lines 28-41),

upon reception of the respond comprising the signature, the data communication apparatus calculates the master secret code (col.7 line 8) based on the chosen algorithm, the signature received and the private key, and establish a secure connection to the wireless communication apparatus (col.6 line 28 thru col.7 line 13).

It would have been obvious to one of ordinary skill in the art to combine Ichikawa's method of generating encryption keys with Anvret et al's means for identification and exchange of encryption keys in order to promote the usage of smart cards that enable strong algorithms and enhanced security (Anvret et al col.1 lines 23-25).

Claims 5,15,19,22-24 are substantially equivalent to claim 1, therefore claims 3,5,15,19,22-24 are rejected because of similar rationale.

Regarding claim 3, Ichikawa and Anvret et al teach a method according to claim 1 further comprising a step of re-establishing the connection by transmitting a request from the wireless communication apparatus to the data communication apparatus, said request comprising the calculated signature based on the chosen algorithm, the public key and the stored secret key (Anvret et al col.6 lines 1-11; col.6 lines 47-48; col.6 lines 39-41), and upon reception of the request, the data communication apparatus calculates the master secret code based on the chosen algorithm, the signature received, and the private key, and, establish a secure connection to the wireless communication apparatus (Anvret et al col.6 line 28 thru col.7 line 13).

Regarding claim 4, Ichikawa and Anvret et al teach a method according to claim 1, in addition Ichikawa teaches a step of providing said separate unit in a smart card (page 2 lines 16-25).

Regarding claim 6, Ichikawa and Anvret et al teach an apparatus according to claim 5, in addition Anvret et al teaches a wireless communication apparatus having its memory means exchangeable (col.2 lines 37-41).

Regarding claim 7, Ichikawa and Anvret et al teach an apparatus according to claim 5, in addition Ichikawa teaches a wireless communication apparatus wherein the master secret code is generated on a separate unit (fig.1; page 4 lines 2-15).

Regarding claim 8, Ichikawa and Anvret et al teach an apparatus according to claims 5 to 7, in addition Ichikawa teaches a wireless communication apparatus wherein the signature is stored on the separate unit (fig.1; page 4 lines 2-15).

Regarding claim 9, Ichikawa and Anvret et al teach an apparatus according to claims 5, in addition Ichikawa teaches a wireless communication apparatus wherein the master secret code is generated on the separate unit (fig.1; page 4 lines 2-15).

Regarding claim 10, Ichikawa and Anvret et al teach an apparatus according to claims 5, in addition Ichikawa teaches a wireless communication apparatus wherein the signature is generated on the separate unit (fig.1; page 4 lines 2-15).

Regarding claim 11, Ichikawa and Anvret et al teach an apparatus according to claim 5, in addition Ichikawa teaches the separate unit comprises a smart card (page 2 lines 16-25).

Regarding claim 12, Ichikawa and Anvret et al teach an apparatus according to claim 11, in addition Ichikawa teaches the smart card is a subscriber identity module (page 2 lines 16-25).

Regarding claim 13, Ichikawa and Anvret et al teach an apparatus according to claim 11, in addition Ichikawa teaches a smart card (page 2 lines 16-25).

Regarding claim 14, Ichikawa and Anvret et al teach an apparatus according to claim 5, in addition Ichikawa teaches a wireless communication apparatus without a smart card (page 2 lines 16-25).

Regarding claim 16, Ichikawa and Anvret et al teach a memory card according to claim 15, in addition Ichikawa teaches encryption means for encrypting the master secret, which is to be used as a signature for the wireless communication apparatus when it is establishing a secure connection (page 11 line 19 thru page 12 line 2).

Regarding claim 17, Ichikawa and Anvret et al teach a memory card according to claim 15, in addition Ichikawa teaches a secure database provided with at least one master secret code and/or at least one signature related to one or more data communication apparatus, in order to re-establish a secure connection to a data communication apparatus (page 4 lines 12-15; fig.5; page 7 line 9 thru page 8 line 10; page 11 line 19 thru page 12 line 2).

Regarding claim 18, Ichikawa and Anvret et al teach a memory card according to claim 15, in addition Ichikawa teaches a memory card provided on a smart card (page 6 lines 15-16).

Regarding claim 21, Ichikawa and Anvret et al teach a system according to claim 19, in addition Ichikawa teaches memory means is a smart card (page 2 line 16 thru page 3 line 12).

Claim 27 is substantially equivalent to claim 4, therefore claim 27 is rejected because of similar rationale.

Claim 28 is substantially equivalent to claim 7, therefore claim 28 is rejected because of similar rationale.

Claims 29-31 are substantially equivalent to claim 9, therefore claim 29-31 are rejected because of similar rationale.

Claims 32-35 are substantially equivalent to claim 10, therefore claim 32-35 are rejected because of similar rationale.

Claims 36-40 are substantially equivalent to claim 11, therefore claim 36-40 are rejected because of similar rationale.

Claim 41 is substantially equivalent to claim 13, therefore claim 41 is rejected because of similar rationale.

Claim 42 is substantially equivalent to claim 17, therefore claim 42 is rejected because of similar rationale.

Claims 43,44 are substantially equivalent to claim 7, therefore claims 43,44 are rejected because of similar rationale.

8. Claims 2,20,25,26,45 rejected under 35 U.S.C. 103(a) as being unpatentable over Ichikawa (PCT WO 97/24831) and Anvret et al (EPO 0538216 A1), and further in view of Weiss (US pat 5,485,519).

Regarding claim 2, Ichikawa and Anvret et al teach a method according to claim 1, but do not teach a step of saving said master secret under a pre-defined time. Weiss teaches a step of saving said master secret under a pre-defined time (col.12 lines 40-61). It would have been obvious to one of ordinary skill in the art to combine Ichikawa and Anvret et al's method of an encryption key exchange with Weiss's teaching of saving keys for a pre-defined time in order to prevent an unauthorized user from compromising the key.

Claim 20 is substantially equivalent to claim 2, therefore claim 20 is rejected because of similar rationale.

Claim 26 is substantially equivalent to claim 4, therefore claim 26 is rejected because of similar rationale.

Claim 45 is substantially equivalent to claim 18, therefore claim 45 is rejected because of similar rationale.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Tremayne M. Norris whose telephone number

Art Unit: 2137

is (703) 305-8045. The examiner can normally be reached on M-F 7:30AM-5:00PM alternate Fridays.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory Morse can be reached on (703) 305-4789. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).


Tremayne Norris

April 16, 2004


MATTHEW SMITHERS
PRIMARY EXAMINER
Art Unit 2137